

**Semester 1 – 2021/2022**

Course Code	CYS613
Course Name	Advanced Principals of Cyber Security
Assignment type	SeedLab
Module	07

Student ID	
Student Name	
CRN	15320

Solution:

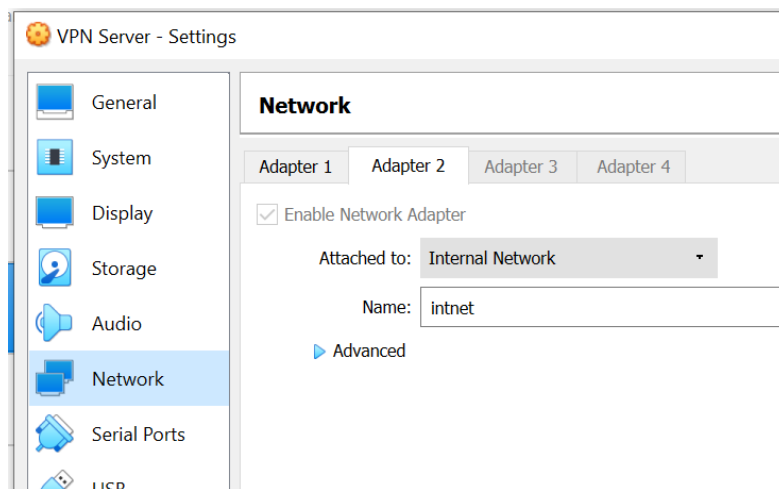
## Virtual Private Network (VPN) Lab

### Lab Setup

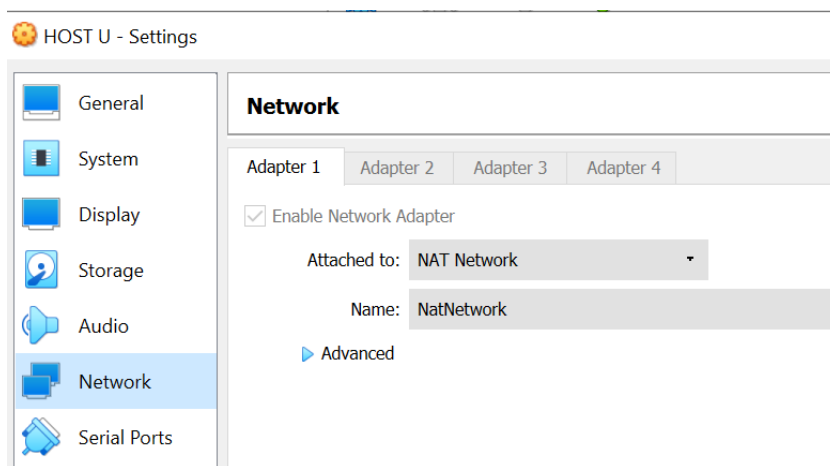
We have three machines in this lab, the VPN server, host U and host V. Host V will be the isolated machine, and we will try to make host U communicate with the isolated machine host V.

First, we will make the environment ready by having three machines and setup the network cards for each machine as follow:

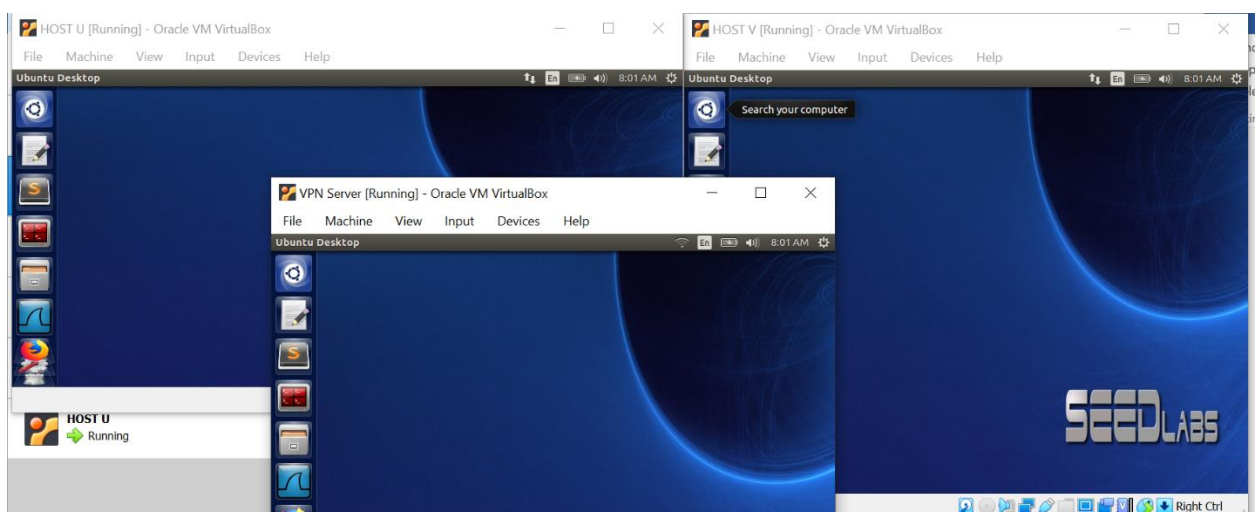
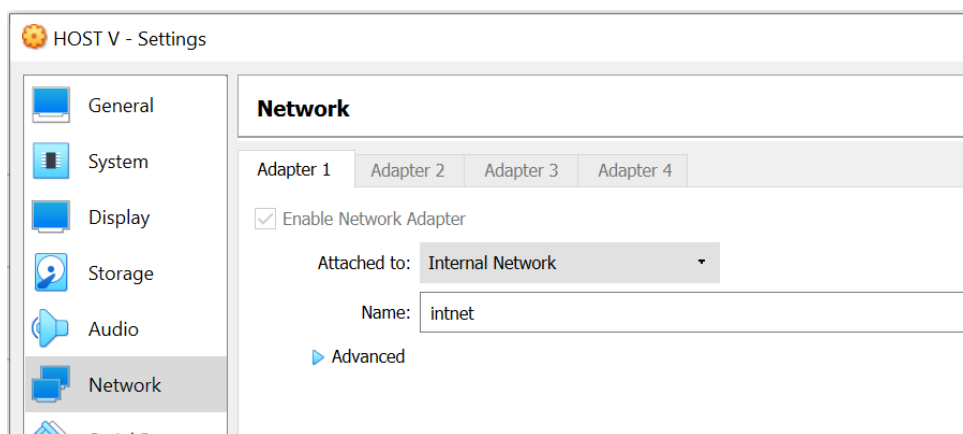
The VPN server will have two Network adapters:



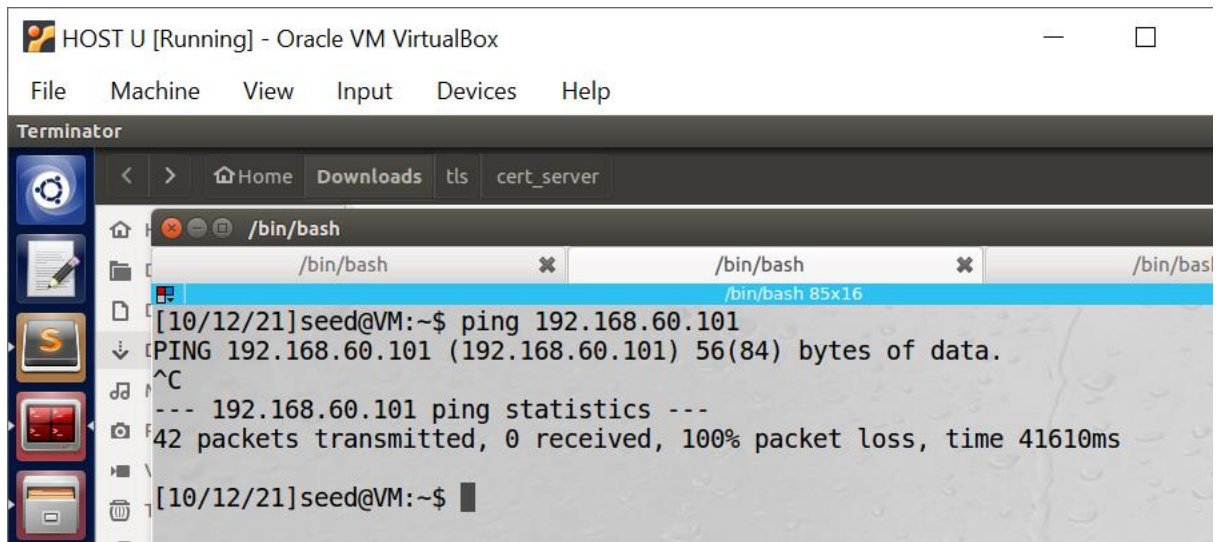
## Host U



## Host V



Host U can't ping host V, and they are not on the same network



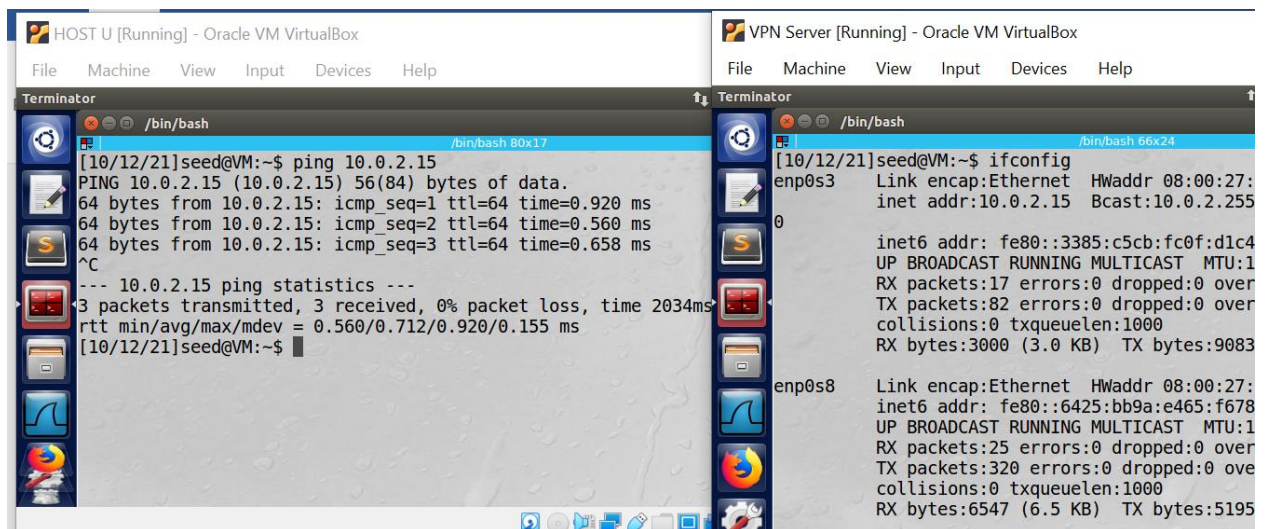
```
HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
< > Home Downloads tls cert_server

/bin/bash
[10/12/21]seed@VM:~$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
^C
--- 192.168.60.101 ping statistics ---
42 packets transmitted, 0 received, 100% packet loss, time 41610ms

[10/12/21]seed@VM:~$
```

Host U can ping the server



```
HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

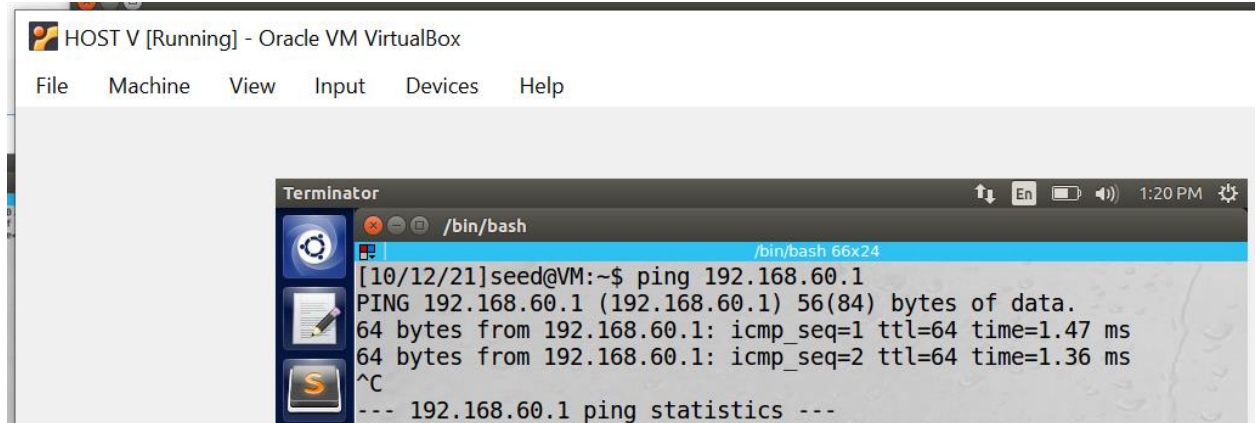
Terminator
/bin/bash
[10/12/21]seed@VM:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.920 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.560 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.658 ms
^C
--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.560/0.712/0.920/0.155 ms
[10/12/21]seed@VM:~$
```

```
VPN Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
[10/12/21]seed@VM:~$ ifconfig
enp0s3: Link encap:Ethernet HWaddr 08:00:27:
        inet addr:10.0.2.15 Bcast:10.0.2.255
        inet6 addr: fe80::3385:c5cb:fc0f:d1c4
        UP BROADCAST RUNNING MULTICAST MTU:1
        RX packets:17 errors:0 dropped:0 over
        TX packets:82 errors:0 dropped:0 over
        collisions:0 txqueuelen:1000
        RX bytes:3000 (3.0 KB) TX bytes:9083

enp0s8: Link encap:Ethernet HWaddr 08:00:27:
        inet6 addr: fe80::6425:bb9a:e465:f678
        UP BROADCAST RUNNING MULTICAST MTU:1
        RX packets:25 errors:0 dropped:0 over
        TX packets:320 errors:0 dropped:0 ove
        collisions:0 txqueuelen:1000
        RX bytes:6547 (6.5 KB) TX bytes:5195
```

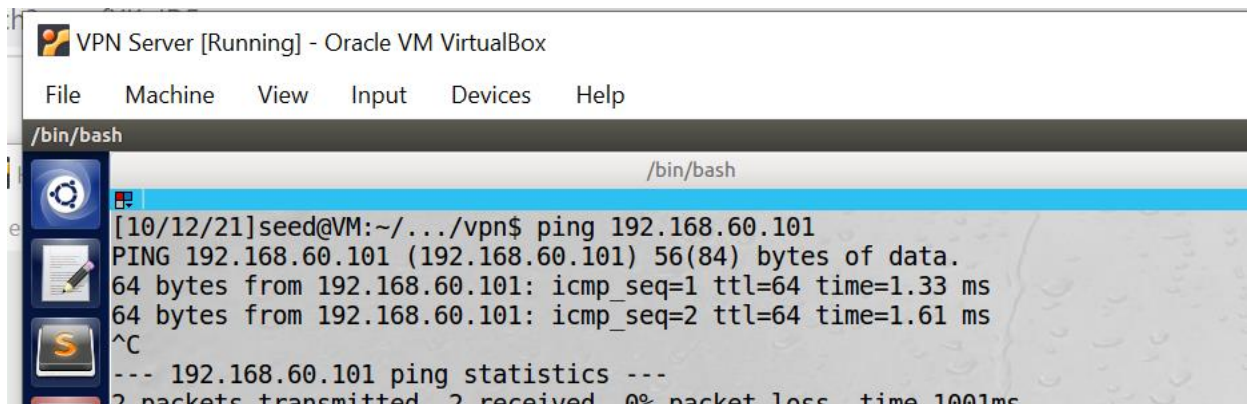
And host V can ping the server



The screenshot shows the Oracle VM VirtualBox interface with the 'HOST V [Running]' window. Inside, a 'Terminator' terminal window is open, displaying a successful ping command from host V to the server at 192.168.60.1. The terminal output shows two successful ping requests with response times of 1.47 ms and 1.36 ms.

```
[10/12/21]seed@VM:~$ ping 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.
64 bytes from 192.168.60.1: icmp_seq=1 ttl=64 time=1.47 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=64 time=1.36 ms
^C
--- 192.168.60.1 ping statistics ---
```

The VPN server can ping the two machines



The screenshot shows the Oracle VM VirtualBox interface with the 'VPN Server [Running]' window. Inside, a 'Terminator' terminal window is open, displaying a successful ping command from the VPN server to the machine at 192.168.60.101. The terminal output shows two successful ping requests with response times of 1.33 ms and 1.61 ms.

```
[10/12/21]seed@VM:~/.../vpn$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
64 bytes from 192.168.60.101: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=64 time=1.61 ms
^C
--- 192.168.60.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
```

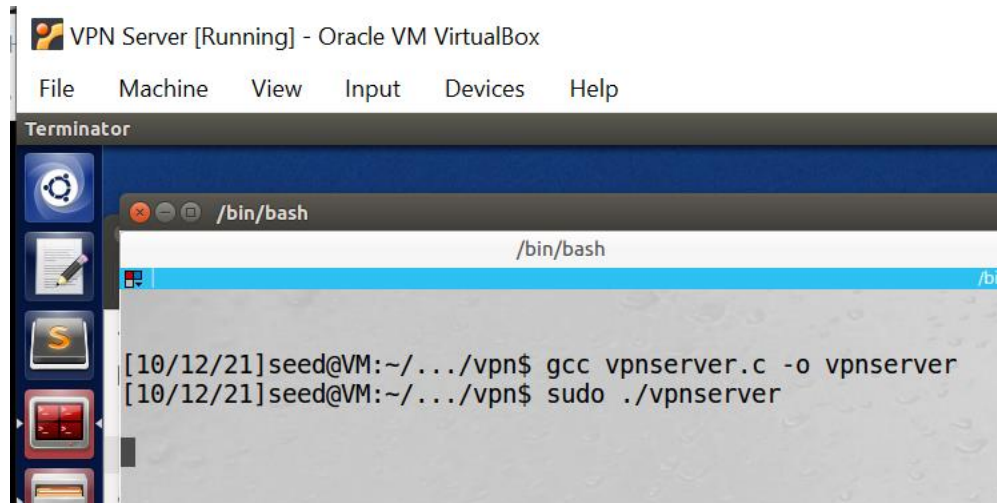
## Task2

### Creating a VPN Tunnel using TUN/TAP

First, download the e VPN client program (vpncclient) and a server program (vpnserv) and unzipped them. The vpncclient and vpnserv programs are the two ends of a VPN tunnel. They communicate with each other using either TCP or UDP via the sockets depicted

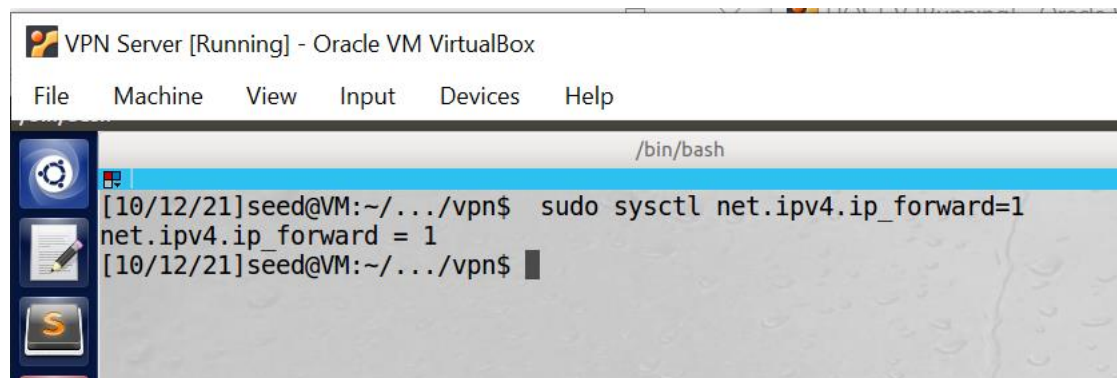
We run VPN Server. We first run the VPN server program `vpnserv` on the Server VM. After the program runs, a virtual TUN network interface will appear in the system.

Compile and run the `vpnserv` in the server machine



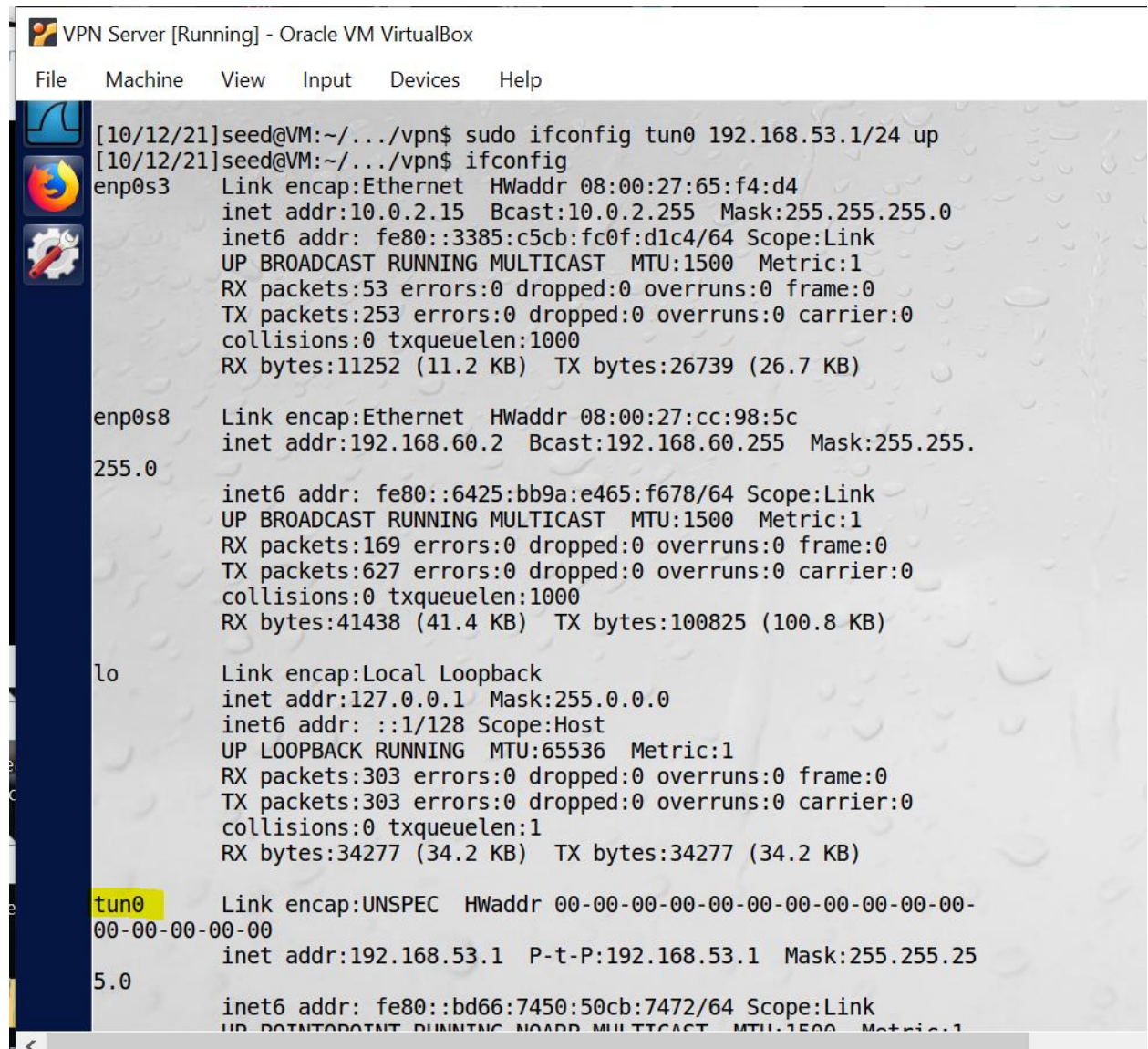
```
VPN Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[10/12/21]seed@VM:~/.../vpn$ gcc vpnserv.c -o vpnserv
[10/12/21]seed@VM:~/.../vpn$ sudo ./vpnserv
```

The VPN Server needs to forward packets between the private network and the tunnel, so it requires to function as a gateway.



```
VPN Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[10/12/21]seed@VM:~/.../vpn$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[10/12/21]seed@VM:~/.../vpn$
```





```

[10/12/21]seed@VM:~/.../vpn$ sudo ifconfig tun0 192.168.53.1/24 up
[10/12/21]seed@VM:~/.../vpn$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:65:f4:d4
            inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::3385:c5cb:fc0f:d1c4/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:53 errors:0 dropped:0 overruns:0 frame:0
            TX packets:253 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:11252 (11.2 KB)  TX bytes:26739 (26.7 KB)

enp0s8      Link encap:Ethernet  HWaddr 08:00:27:cc:98:5c
            inet addr:192.168.60.2  Bcast:192.168.60.255  Mask:255.255.
            255.0
            inet6 addr: fe80::6425:bb9a:e465:f678/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:169 errors:0 dropped:0 overruns:0 frame:0
            TX packets:627 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:41438 (41.4 KB)  TX bytes:100825 (100.8 KB)

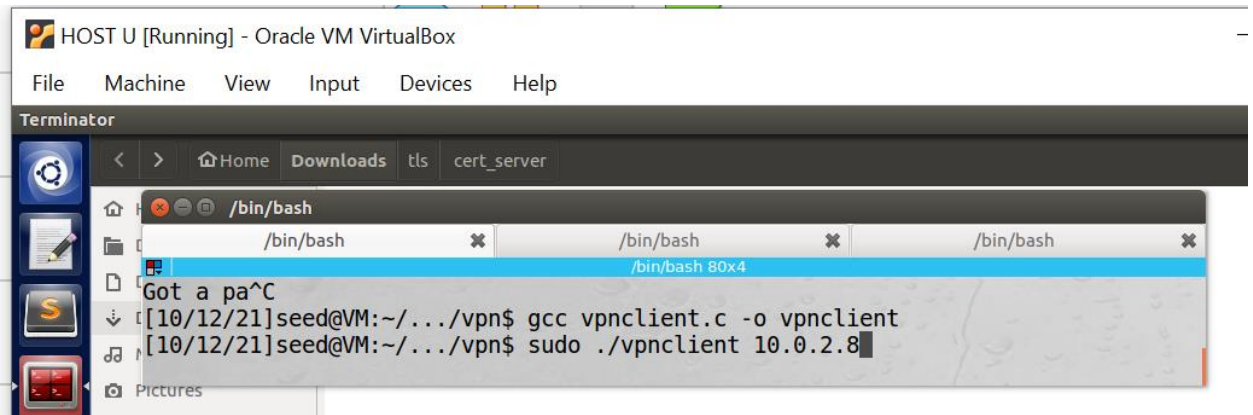
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:303 errors:0 dropped:0 overruns:0 frame:0
            TX packets:303 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:34277 (34.2 KB)  TX bytes:34277 (34.2 KB)

tun0       Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-
            00-00-00-00-00
            inet addr:192.168.53.1  P-t-P:192.168.53.1  Mask:255.255.25
            5.0
            inet6 addr: fe80::bd66:7450:50cb:7472/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

```

Then Run VPN Client. We now run the VPN client program on the Client VM machine

U using the downloaded program

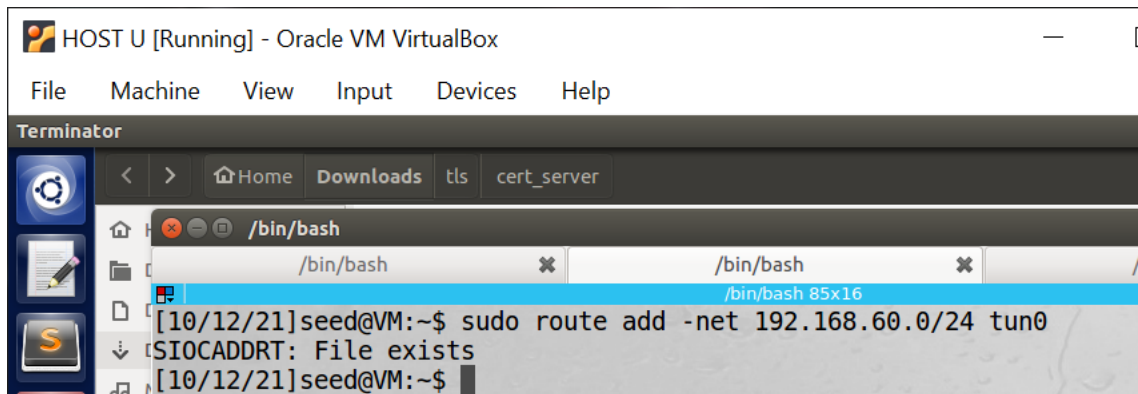


```
HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
< > Home Downloads tls cert_server

/bin/bash
Got a pa^C
[10/12/21]seed@VM:~/.../vpn$ gcc vpnclient.c -o vpnclient
[10/12/21]seed@VM:~/.../vpn$ sudo ./vpnclient 10.0.2.8
```

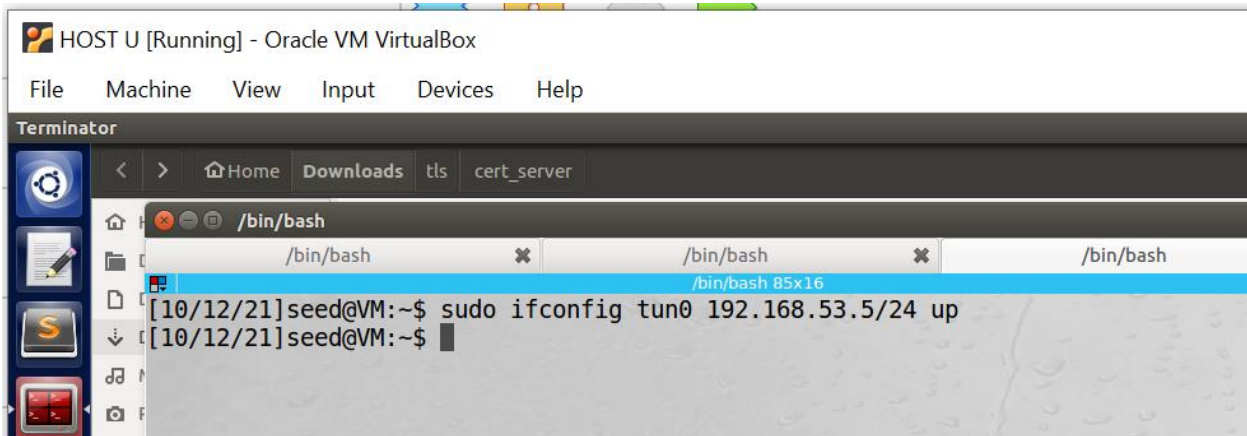
### Set Up Routing on Client and Server VMs



```
HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
< > Home Downloads tls cert_server

/bin/bash
[10/12/21]seed@VM:~$ sudo route add -net 192.168.60.0/24 tun0
SIOCADDRT: File exists
[10/12/21]seed@VM:~$
```

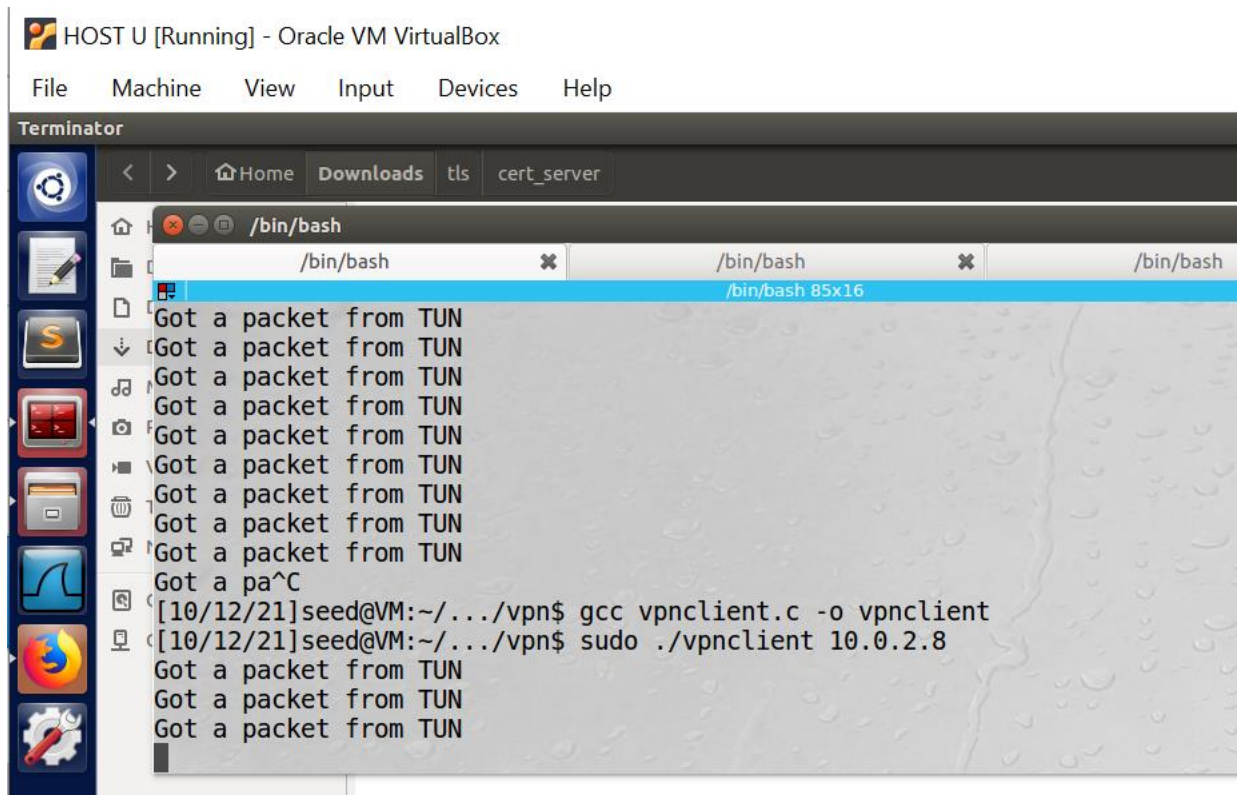


```
HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

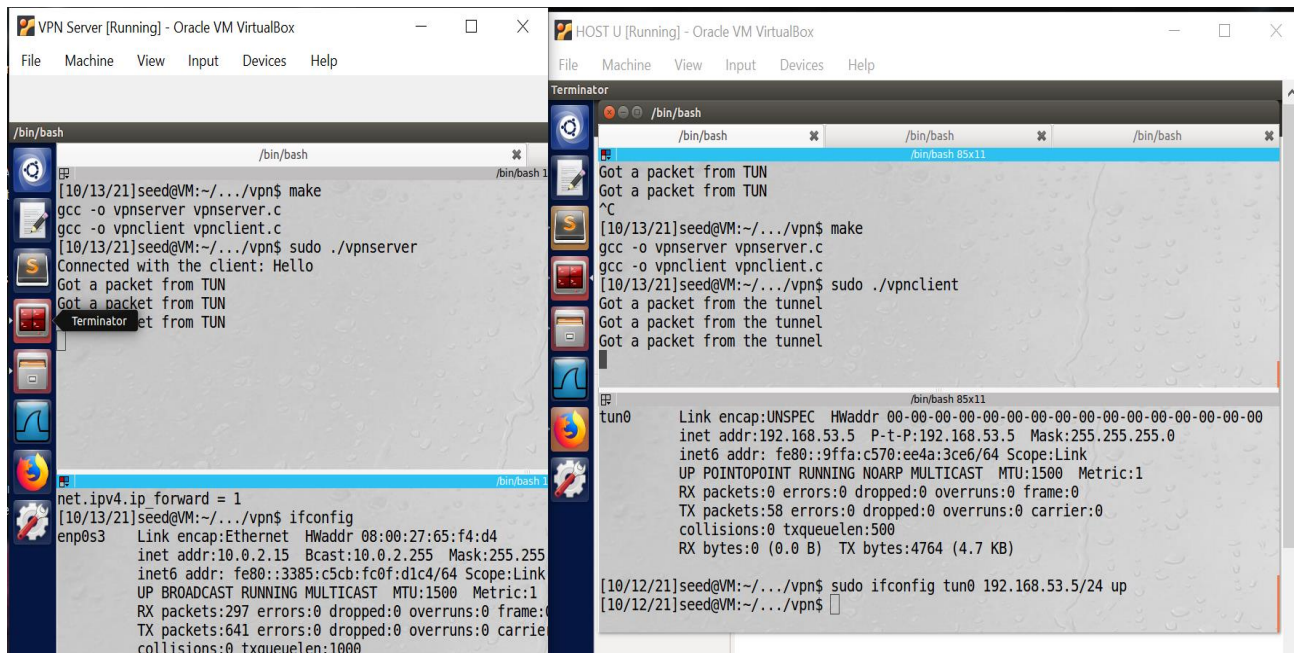
Terminator
< > Home Downloads tls cert_server

/bin/bash
[10/12/21]seed@VM:~$ sudo ifconfig tun0 192.168.53.5/24 up
[10/12/21]seed@VM:~$
```





Here are the two machines the sever and machine U



Test the VPN Tunnel by trying to ping the machine V from the machine U while they are not on the same network

The screenshot shows two Oracle VM VirtualBox windows. The left window, titled 'VPN Server [Running]', shows a terminal with the following output:

```
/bin/bash
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
net.ipv4.ip_forward = 1
[10/13/21]seed@VM:~/.../vpn$ sudo ifconfig tun0 192.168.53.5/24 up
[10/13/21]seed@VM:~/.../vpn$ sudo route add -net 192.168.60.0/24 tun0
[10/13/21]seed@VM:~/.../vpn$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data:
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=1.90 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=2.53 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=1.64 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=2.03 ms
^C
--- 192.168.60.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.646/2.030/2.530/0.324 ms
[10/13/21]seed@VM:~/.../vpn$
```

The right window, titled 'HOST U [Running]', shows a terminal with the following output:

```
/bin/bash
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
[10/13/21]seed@VM:~/.../vpn$ sudo ifconfig tun0 192.168.53.5/24 up
[10/13/21]seed@VM:~/.../vpn$ sudo route add -net 192.168.60.0/24 tun0
[10/13/21]seed@VM:~/.../vpn$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data:
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=1.90 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=2.53 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=1.64 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=2.03 ms
^C
--- 192.168.60.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.646/2.030/2.530/0.324 ms
[10/13/21]seed@VM:~/.../vpn$
```

And telnet the machine V from machine U

The screenshot shows two Oracle VM VirtualBox windows. The left window, titled 'VPN Server [Running]', shows a terminal with the following output:

```
/bin/bash
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
net.ipv4.ip_forward = 1
[10/13/21]seed@VM:~/.../vpn$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:65:f4:d4
inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255
inet6 addr: fe80::3385:c5cb:fc0f:d1c4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:297 errors:0 dropped:0 overruns:0 frame:0
TX packets:641 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:77588 (77.5 KB) TX bytes:93166 (93.1 KB)

enp0s8 Link encap:Ethernet HWaddr 08:00:27:cc:98:5c
inet addr:192.168.60.1 Bcast:192.168.60.255 Mask:255.255.255
inet6 addr: fe80::6425:bb9a:e465:f678/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

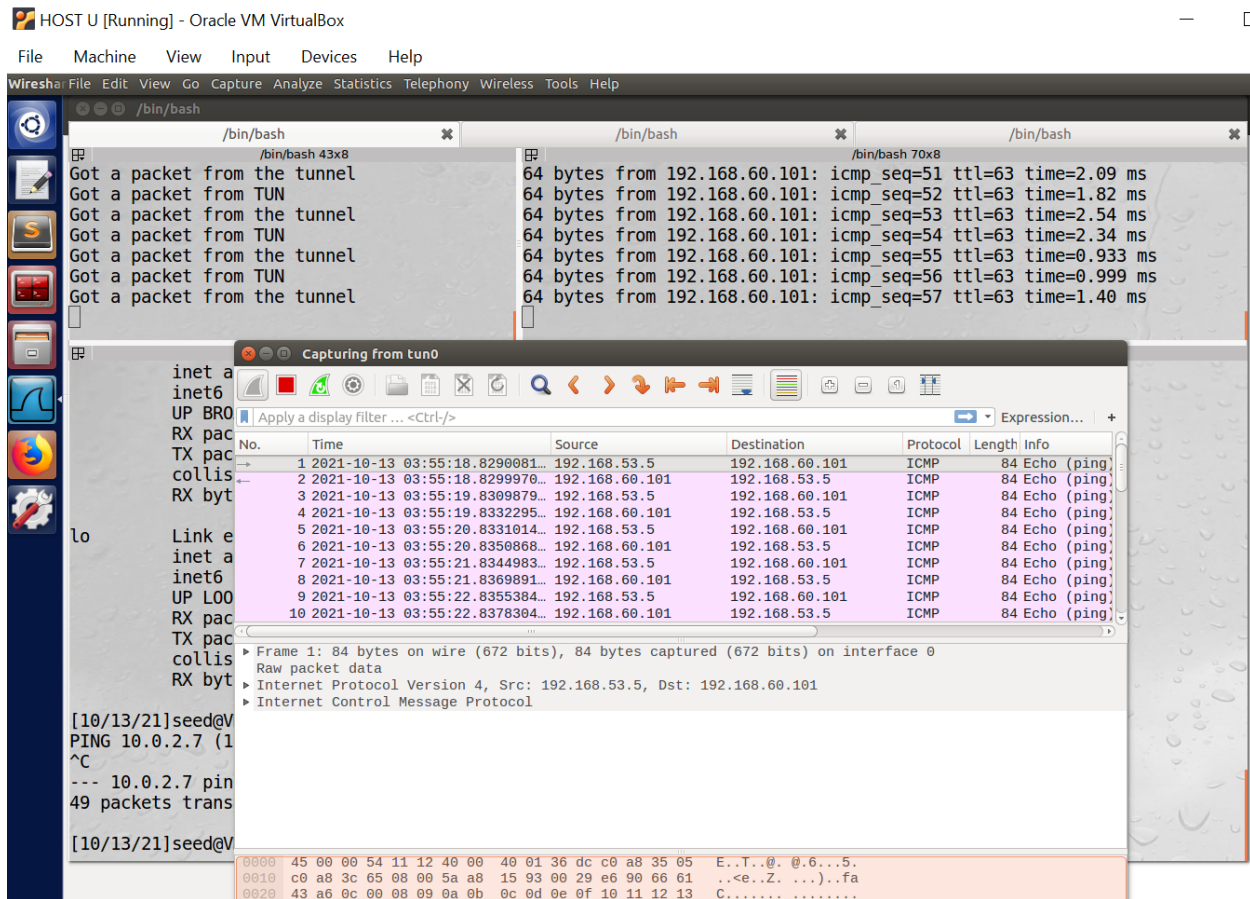
The right window, titled 'HOST U [Running]', shows a terminal with the following output:

```
/bin/bash
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
[10/13/21]seed@VM:~/.../vpn$ telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Apr 3 02:20:24 EDT 2021 from 10.0.2.7 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic 1686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.
[10/13/21]seed@VM:~/.../vpn$
```

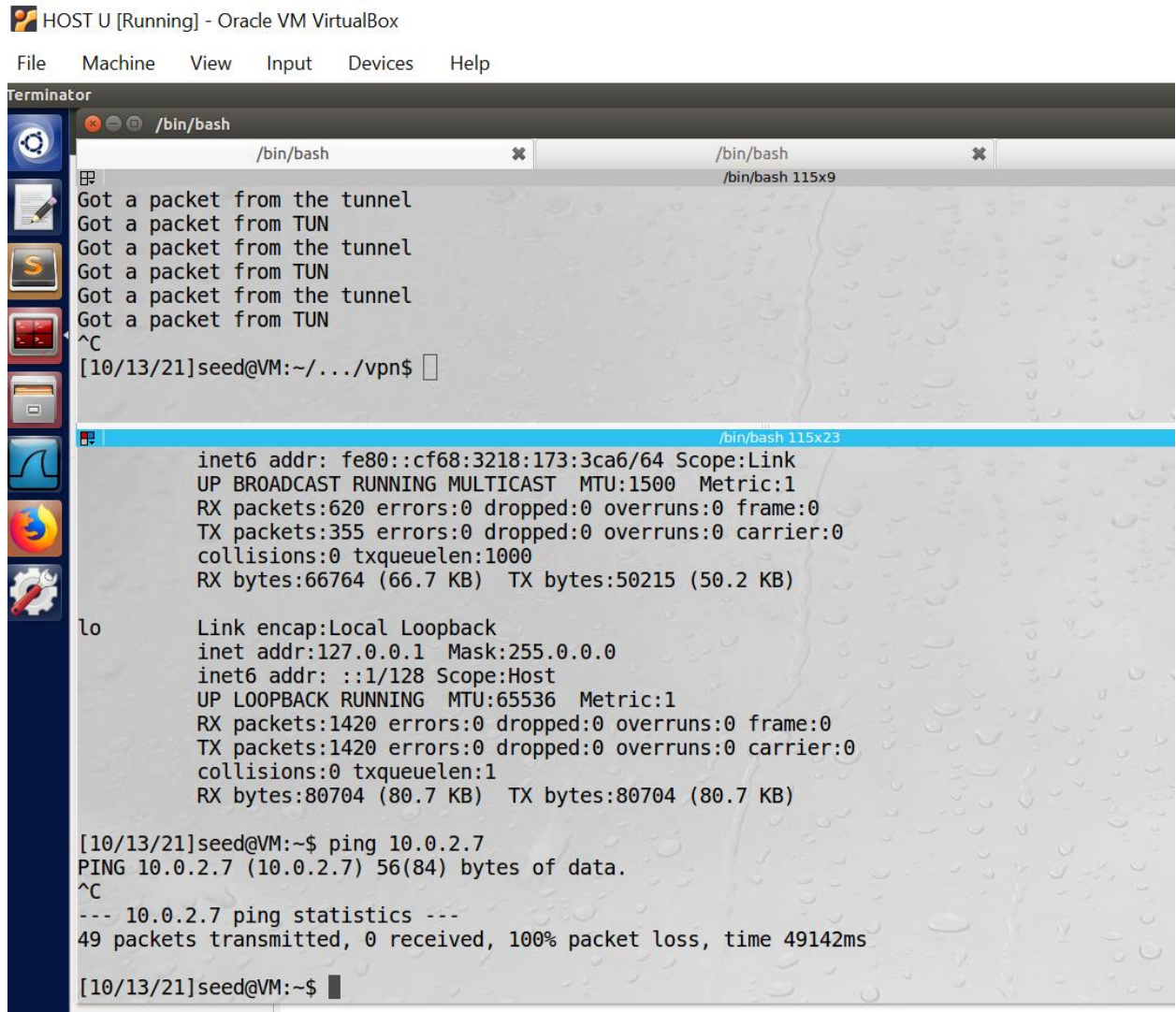
Wireshark to capture the network traffics on all the interfaces on the client VM



Tunnel-Breaking Test.

After breaking the tunnel, we can't access machine V from machine U





```
HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
^C
[10/13/21]seed@VM:~/.../vpn$

/bin/bash 115x23
inet6 addr: fe80::cf68:3218:173:3ca6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:620 errors:0 dropped:0 overruns:0 frame:0
TX packets:355 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:66764 (66.7 KB) TX bytes:50215 (50.2 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:1420 errors:0 dropped:0 overruns:0 frame:0
TX packets:1420 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:80704 (80.7 KB) TX bytes:80704 (80.7 KB)

[10/13/21]seed@VM:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
^C
--- 10.0.2.7 ping statistics ---
49 packets transmitted, 0 received, 100% packet loss, time 49142ms

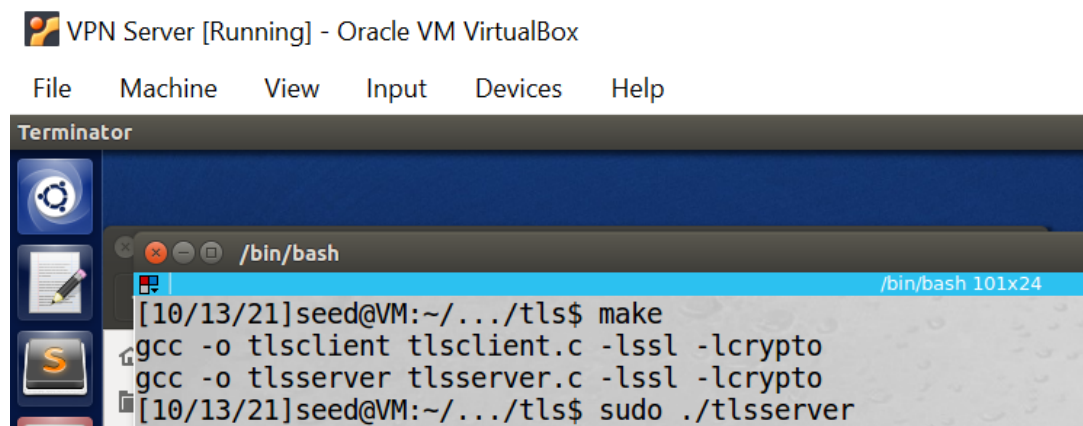
[10/13/21]seed@VM:~$
```

### Task 3 and 4: Encrypting the Tunnel, Authenticating the VPN Server

To secure this tunnel, we need to achieve two goals, confidentiality and integrity. The confidentiality is achieved using encryption, i.e., the contents that go through the tunnel is encrypted. The integrity goal ensures that nobody can tamper with the traffic in the tunnel or launch a replay attack. Integrity can be achieved using Message Authentication Code (MAC)

A sample TLS client and server program (tlsclient and tlsserver) is provided in a zip file that can be downloaded from the website

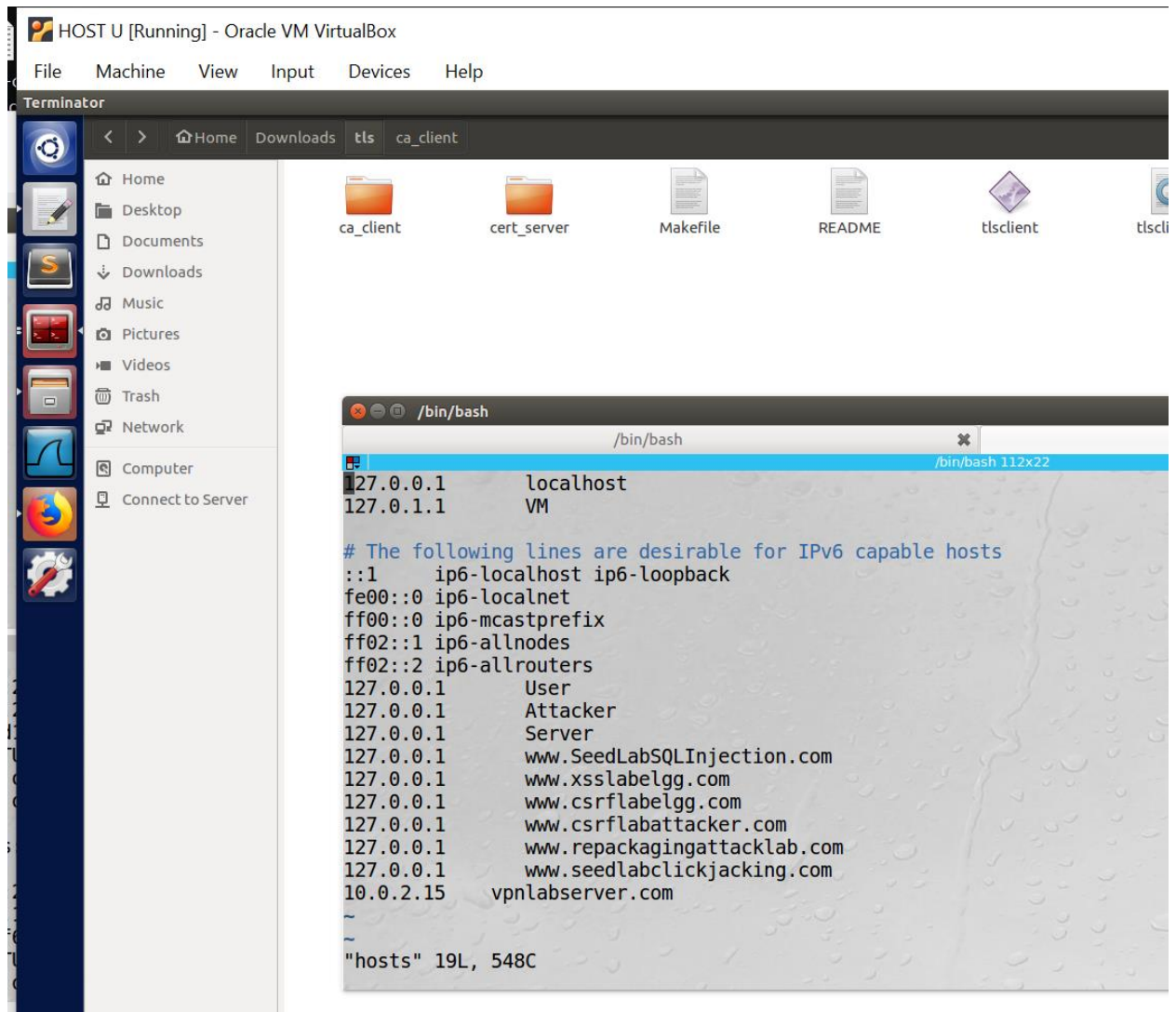
On the Server machine we compile and run the tlsserver program



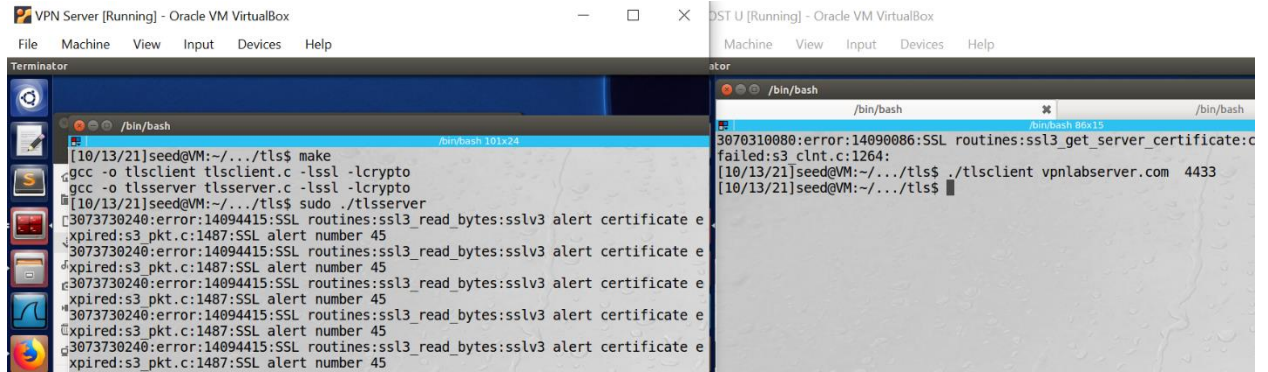
```
VPN Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[10/13/21]seed@VM:~/.../tls$ make
gcc -o tlsclient tlsclient.c -lssl -lcrypto
gcc -o tlsserver tlsserver.c -lssl -lcrypto
[10/13/21]seed@VM:~/.../tls$ sudo ./tlsserver
```



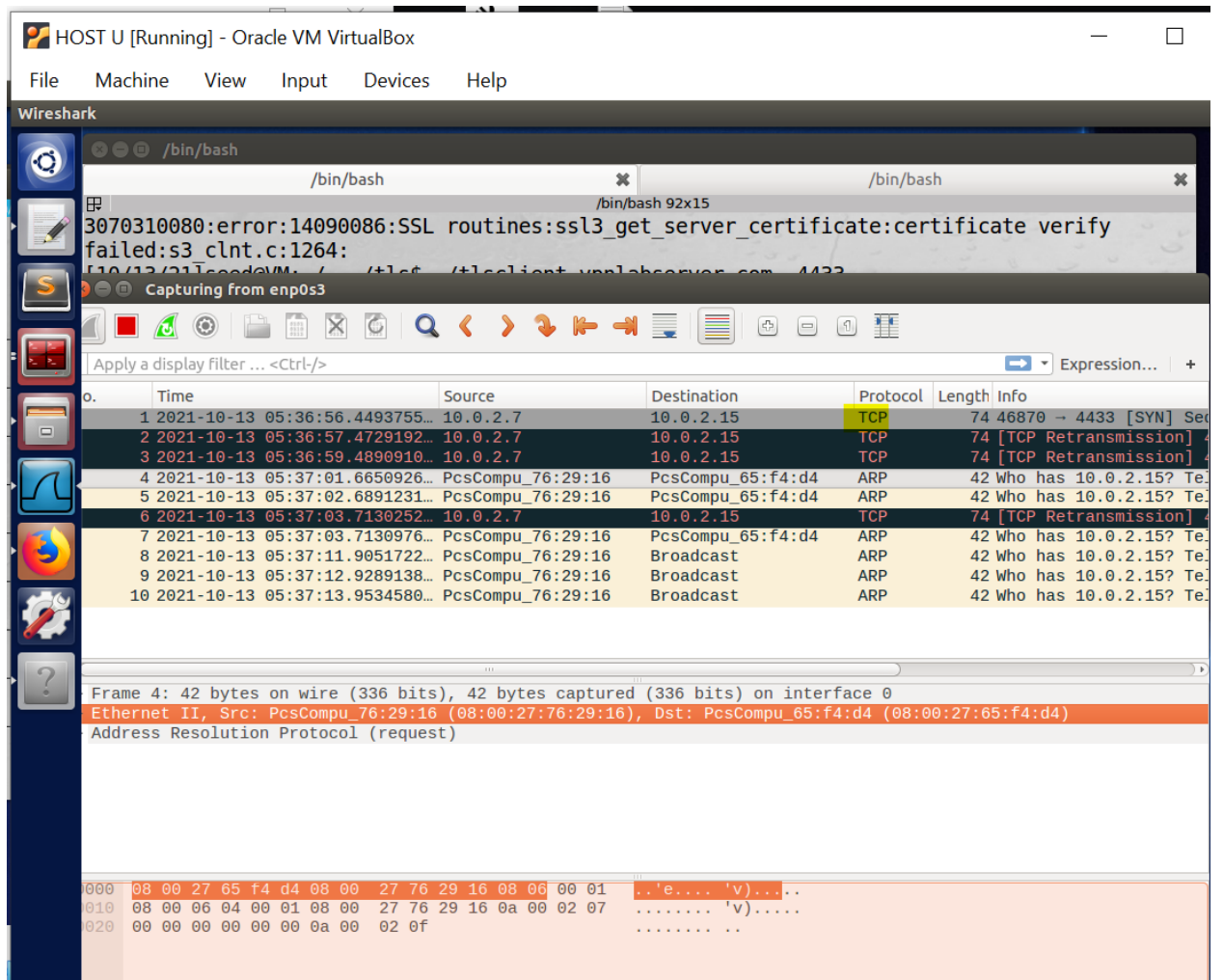
On the host U machine, we should first read the “read me” file to add the server IP and hostname to /etc/hosts as mentions in the file



Then after that we use the command that mentioned in the file and run the `tlsclient` program

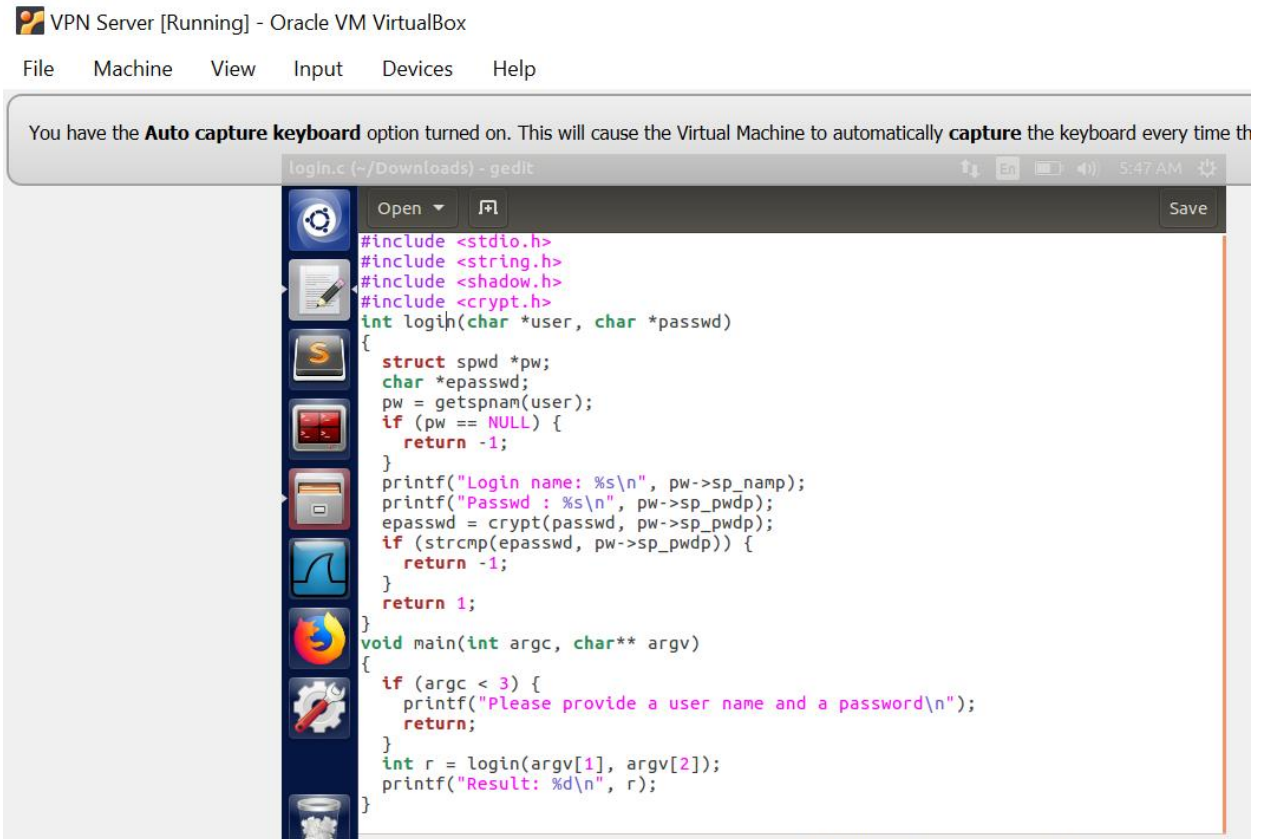


Start the wireshark to capture the network



## Task 5: Authenticating the VPN Client

Here are the code

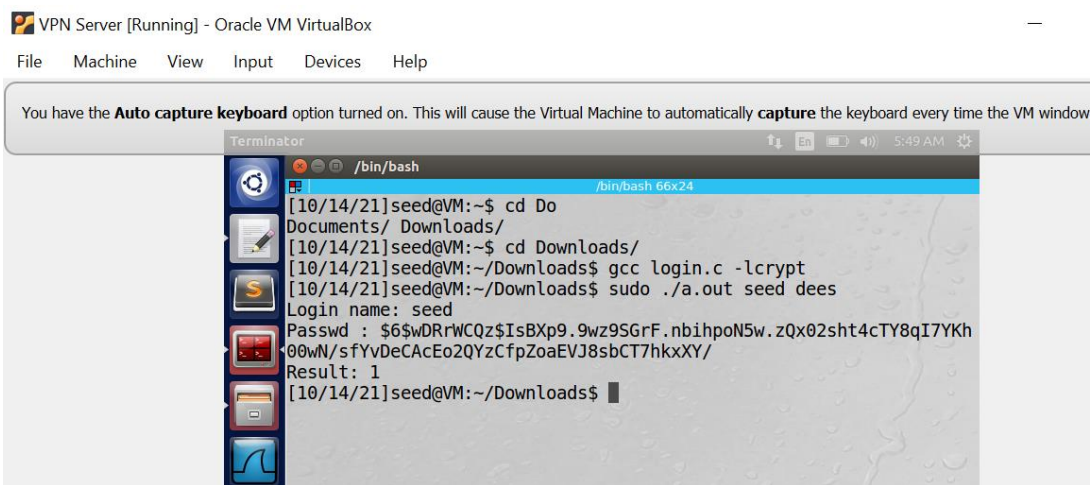


The screenshot shows a virtual machine window titled "VPN Server [Running] - Oracle VM VirtualBox". The menu bar includes File, Machine, View, Input, Devices, and Help. A message at the top states: "You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is active." The main area displays a code editor with the file "login.c (~/.Downloads) - gedit". The code is as follows:

```
#include <stdio.h>
#include <string.h>
#include <shadow.h>
#include <crypt.h>
int login(char *user, char *passwd)
{
    struct spwd *pw;
    char *epasswd;
    pw = getspnam(user);
    if (pw == NULL) {
        return -1;
    }
    printf("Login name: %s\n", pw->sp_namp);
    printf("Passwd : %s\n", pw->sp_pwdp);
    epasswd = crypt(passwd, pw->sp_pwdp);
    if (strcmp(epasswd, pw->sp_pwdp)) {
        return -1;
    }
    return 1;
}
void main(int argc, char** argv)
{
    if (argc < 3) {
        printf("Please provide a user name and a password\n");
        return;
    }
    int r = login(argv[1], argv[2]);
    printf("Result: %d\n", r);
}
```

We can compile the code above and run it with a user name and a password.

We use the seed and dees as password and username



The screenshot shows the same virtual machine window. The main area displays a terminal window titled "Terminator". The terminal output is as follows:

```
/bin/bash
[10/14/21]seed@VM:~$ cd Do
Documents/ Downloads/
[10/14/21]seed@VM:~$ cd Downloads/
[10/14/21]seed@VM:~/Downloads$ gcc login.c -lcrypt
[10/14/21]seed@VM:~/Downloads$ sudo ./a.out seed dees
Login name: seed
Passwd : $6$wDRrWCQzIsBXp9.9wz9SGrF.nbihpoN5w.zQx02sht4cTY8qI7YKh
00wN/sfYvDeCacEo2QYzCfpZoaEVJ8sbCT7hkkXY/
Result: 1
[10/14/21]seed@VM:~/Downloads$
```

## Task 6: Supporting Multiple Clients

Linux has a system call called `select()`, which allows a program to monitor multiple file descriptors simultaneously

```
fd_set readFDSet;
int ret, sockfd, tunfd;

FD_ZERO(&readFDSet);
FD_SET(sockfd, &readFDSet);           ①
FD_SET(tunfd, &readFDSet);           ②
ret = select(FD_SETSIZE, &readFDSet, NULL, NULL, NULL); ③

if (FD_ISSET(sockfd, &readFDSet){
    // Read data from sockfd, and do something.
}

if (FD_ISSET(tunfd, &readFDSet){
    // Read data from tunfd, and do something.
}
```